

AMENDED IN SENATE APRIL 22, 2015

SENATE BILL

No. 34

Introduced by Senator Hill

December 1, 2014

An act to amend Sections 1798.29 and 1798.82 of, and to add Title 1.81.23 (commencing with Section 1798.90.5) to Part 4 of Division 3 of, the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 34, as amended, Hill. Automated license plate recognition systems: use of data.

(1) Existing law authorizes the Department of the California Highway Patrol to retain license plate data captured by license plate recognition (LPR) technology, also referred to as an automated license plate recognition (ALPR) system, for not more than 60 days unless the data is being used as evidence or for the investigation of felonies. Existing law prohibits the department from selling the data or from making the data available to an agency that is not a law enforcement agency or an individual that is not a law enforcement officer.

Existing law authorizes the department to use LPR data for the purpose of locating vehicles or persons reasonably suspected of being involved in the commission of a public offense, and requires the department to monitor the internal use of the data to prevent unauthorized use and to submit to the Legislature, as a part of the annual automobile theft report, information on the department's LPR practices and usage.

This bill would impose specified requirements on an "ALPR operator" as defined, including, among others, ensuring that the information the ALPR operator collects is protected with certain safeguards, and

implementing and maintaining specified security procedures and a usage and privacy policy with respect to that information.

The bill would require an ALPR operator that accesses or provides access to ALPR information to maintain a specified record of that access.

This bill would also require an “ALPR end-user,” as defined, to implement and maintain a specified usage and privacy policy.

The bill would, in addition to any other sanctions, penalties, or remedies provided by law, authorize an individual who has been harmed by a violation of these provisions to bring a civil action in any court of competent jurisdiction against a person who knowingly caused that violation.

The bill would require a public agency that considers implementing a program to gather information through the use of an ALPR system to provide an opportunity for public comment at a regularly scheduled public meeting of the governing body of the public agency before it implements the program.

(2) Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the system or data, as defined, following discovery or notification of the security breach, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Existing law defines “personal information” for these purposes to include an individual’s first name and last name, or first initial and last name, in combination with one or more designated data elements relating to, among other things, social security numbers, driver’s license numbers, financial accounts, and medical information.

This bill would include information or data collected through the use or operation of an automated license plate recognition system, when that information is not encrypted and is used in combination with an individual’s name, in the definition of “personal information” discussed above.

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: no.

The people of the State of California do enact as follows:

1 SECTION 1. Section 1798.29 of the Civil Code is amended
2 to read:

1 1798.29. (a) Any agency that owns or licenses computerized
2 data that includes personal information shall disclose any breach
3 of the security of the system following discovery or notification
4 of the breach in the security of the data to any resident of California
5 whose unencrypted personal information was, or is reasonably
6 believed to have been, acquired by an unauthorized person. The
7 disclosure shall be made in the most expedient time possible and
8 without unreasonable delay, consistent with the legitimate needs
9 of law enforcement, as provided in subdivision (c), or any measures
10 necessary to determine the scope of the breach and restore the
11 reasonable integrity of the data system.

12 (b) Any agency that maintains computerized data that includes
13 personal information that the agency does not own shall notify the
14 owner or licensee of the information of any breach of the security
15 of the data immediately following discovery, if the personal
16 information was, or is reasonably believed to have been, acquired
17 by an unauthorized person.

18 (c) The notification required by this section may be delayed if
19 a law enforcement agency determines that the notification will
20 impede a criminal investigation. The notification required by this
21 section shall be made after the law enforcement agency determines
22 that it will not compromise the investigation.

23 (d) Any agency that is required to issue a security breach
24 notification pursuant to this section shall meet all of the following
25 requirements:

26 (1) The security breach notification shall be written in plain
27 language.

28 (2) The security breach notification shall include, at a minimum,
29 the following information:

30 (A) The name and contact information of the reporting agency
31 subject to this section.

32 (B) A list of the types of personal information that were or are
33 reasonably believed to have been the subject of a breach.

34 (C) If the information is possible to determine at the time the
35 notice is provided, then any of the following: (i) the date of the
36 breach, (ii) the estimated date of the breach, or (iii) the date range
37 within which the breach occurred. The notification shall also
38 include the date of the notice.

1 (D) Whether the notification was delayed as a result of a law
2 enforcement investigation, if that information is possible to
3 determine at the time the notice is provided.

4 (E) A general description of the breach incident, if that
5 information is possible to determine at the time the notice is
6 provided.

7 (F) The toll-free telephone numbers and addresses of the major
8 credit reporting agencies, if the breach exposed a social security
9 number or a driver's license or California identification card
10 number.

11 (3) At the discretion of the agency, the security breach
12 notification may also include any of the following:

13 (A) Information about what the agency has done to protect
14 individuals whose information has been breached.

15 (B) Advice on steps that the person whose information has been
16 breached may take to protect himself or herself.

17 (4) In the case of a breach of the security of the system involving
18 personal information defined in paragraph (2) of subdivision (g)
19 for an online account, and no other personal information defined
20 in paragraph (1) of subdivision (g), the agency may comply with
21 this section by providing the security breach notification in
22 electronic or other form that directs the person whose personal
23 information has been breached to promptly change his or her
24 password and security question or answer, as applicable, or to take
25 other steps appropriate to protect the online account with the
26 agency and all other online accounts for which the person uses the
27 same user name or email address and password or security question
28 or answer.

29 (5) In the case of a breach of the security of the system involving
30 personal information defined in paragraph (2) of subdivision (g)
31 for login credentials of an email account furnished by the agency,
32 the agency shall not comply with this section by providing the
33 security breach notification to that email address, but may, instead,
34 comply with this section by providing notice by another method
35 described in subdivision (i) or by clear and conspicuous notice
36 delivered to the resident online when the resident is connected to
37 the online account from an Internet Protocol address or online
38 location from which the agency knows the resident customarily
39 accesses the account.

1 (e) Any agency that is required to issue a security breach
2 notification pursuant to this section to more than 500 California
3 residents as a result of a single breach of the security system shall
4 electronically submit a single sample copy of that security breach
5 notification, excluding any personally identifiable information, to
6 the Attorney General. A single sample copy of a security breach
7 notification shall not be deemed to be within subdivision (f) of
8 Section 6254 of the Government Code.

9 (f) For purposes of this section, “breach of the security of the
10 system” means unauthorized acquisition of computerized data that
11 compromises the security, confidentiality, or integrity of personal
12 information maintained by the agency. Good faith acquisition of
13 personal information by an employee or agent of the agency for
14 the purposes of the agency is not a breach of the security of the
15 system, provided that the personal information is not used or
16 subject to further unauthorized disclosure.

17 (g) For purposes of this section, “personal information” means
18 either of the following:

19 (1) An individual’s first name or first initial and last name in
20 combination with any one or more of the following data elements,
21 when either the name or the data elements are not encrypted:

22 (A) Social security number.

23 (B) Driver’s license number or California identification card
24 number.

25 (C) Account number, credit or debit card number, in
26 combination with any required security code, access code, or
27 password that would permit access to an individual’s financial
28 account.

29 (D) Medical information.

30 (E) Health insurance information.

31 (F) Information or data collected through the use or operation
32 of an automated license plate recognition system, as defined in
33 Section 1798.90.5.

34 (2) A user name or email address, in combination with a
35 password or security question and answer that would permit access
36 to an online account.

37 (h) (1) For purposes of this section, “personal information”
38 does not include publicly available information that is lawfully
39 made available to the general public from federal, state, or local
40 government records.

(2) For purposes of this section, “medical information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, “health insurance information” means an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.

(i) For purposes of this section, “notice” may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the agency has an email address for the subject persons.

(B) Conspicuous posting of the notice on the agency’s Internet Web site page, if the agency maintains one.

(C) Notification to major statewide media and the Office of Information Security within the Department of Technology.

(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(k) Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, “agency” includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code.

SEC. 2. Section 1798.82 of the Civil Code is amended to read:

1 1798.82. (a) A person or business that conducts business in
2 California, and that owns or licenses computerized data that
3 includes personal information, shall disclose a breach of the
4 security of the system following discovery or notification of the
5 breach in the security of the data to a resident of California whose
6 unencrypted personal information was, or is reasonably believed
7 to have been, acquired by an unauthorized person. The disclosure
8 shall be made in the most expedient time possible and without
9 unreasonable delay, consistent with the legitimate needs of law
10 enforcement, as provided in subdivision (c), or any measures
11 necessary to determine the scope of the breach and restore the
12 reasonable integrity of the data system.

13 (b) A person or business that maintains computerized data that
14 includes personal information that the person or business does not
15 own shall notify the owner or licensee of the information of the
16 breach of the security of the data immediately following discovery,
17 if the personal information was, or is reasonably believed to have
18 been, acquired by an unauthorized person.

19 (c) The notification required by this section may be delayed if
20 a law enforcement agency determines that the notification will
21 impede a criminal investigation. The notification required by this
22 section shall be made promptly after the law enforcement agency
23 determines that it will not compromise the investigation.

24 (d) A person or business that is required to issue a security
25 breach notification pursuant to this section shall meet all of the
26 following requirements:

27 (1) The security breach notification shall be written in plain
28 language.

29 (2) The security breach notification shall include, at a minimum,
30 the following information:

31 (A) The name and contact information of the reporting person
32 or business subject to this section.

33 (B) A list of the types of personal information that were or are
34 reasonably believed to have been the subject of a breach.

35 (C) If the information is possible to determine at the time the
36 notice is provided, then any of the following: (i) the date of the
37 breach, (ii) the estimated date of the breach, or (iii) the date range
38 within which the breach occurred. The notification shall also
39 include the date of the notice.

1 (D) Whether notification was delayed as a result of a law
2 enforcement investigation, if that information is possible to
3 determine at the time the notice is provided.

4 (E) A general description of the breach incident, if that
5 information is possible to determine at the time the notice is
6 provided.

7 (F) The toll-free telephone numbers and addresses of the major
8 credit reporting agencies if the breach exposed a social security
9 number or a driver's license or California identification card
10 number.

11 (G) If the person or business providing the notification was the
12 source of the breach, an offer to provide appropriate identity theft
13 prevention and mitigation services, if any, shall be provided at no
14 cost to the affected person for not less than 12 months, along with
15 all information necessary to take advantage of the offer to any
16 person whose information was or may have been breached if the
17 breach exposed or may have exposed personal information defined
18 in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

19 (3) At the discretion of the person or business, the security
20 breach notification may also include any of the following:

21 (A) Information about what the person or business has done to
22 protect individuals whose information has been breached.

23 (B) Advice on steps that the person whose information has been
24 breached may take to protect himself or herself.

25 (4) In the case of a breach of the security of the system involving
26 personal information defined in paragraph (2) of subdivision (h)
27 for an online account, and no other personal information defined
28 in paragraph (1) of subdivision (h), the person or business may
29 comply with this section by providing the security breach
30 notification in electronic or other form that directs the person whose
31 personal information has been breached promptly to change his
32 or her password and security question or answer, as applicable, or
33 to take other steps appropriate to protect the online account with
34 the person or business and all other online accounts for which the
35 person whose personal information has been breached uses the
36 same user name or email address and password or security question
37 or answer.

38 (5) In the case of a breach of the security of the system involving
39 personal information defined in paragraph (2) of subdivision (h)
40 for login credentials of an email account furnished by the person

or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in subdivision (j) or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, “personal information” means either of the following:

(1) An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

1 (B) Driver's license number or California identification card
2 number.

3 (C) Account number, credit or debit card number, in
4 combination with any required security code, access code, or
5 password that would permit access to an individual's financial
6 account.

7 (D) Medical information.

8 (E) Health insurance information.

9 (F) Information or data collected through the use or operation
10 of an automated license plate recognition system, as defined in
11 Section 1798.90.5.

12 (2) A user name or email address, in combination with a
13 password or security question and answer that would permit access
14 to an online account.

15 (i) (1) For purposes of this section, "personal information" does
16 not include publicly available information that is lawfully made
17 available to the general public from federal, state, or local
18 government records.

19 (2) For purposes of this section, "medical information" means
20 any information regarding an individual's medical history, mental
21 or physical condition, or medical treatment or diagnosis by a health
22 care professional.

23 (3) For purposes of this section, "health insurance information"
24 means an individual's health insurance policy number or subscriber
25 identification number, any unique identifier used by a health insurer
26 to identify the individual, or any information in an individual's
27 application and claims history, including any appeals records.

28 (j) For purposes of this section, "notice" may be provided by
29 one of the following methods:

30 (1) Written notice.

31 (2) Electronic notice, if the notice provided is consistent with
32 the provisions regarding electronic records and signatures set forth
33 in Section 7001 of Title 15 of the United States Code.

34 (3) Substitute notice, if the person or business demonstrates that
35 the cost of providing notice would exceed two hundred fifty
36 thousand dollars (\$250,000), or that the affected class of subject
37 persons to be notified exceeds 500,000, or the person or business
38 does not have sufficient contact information. Substitute notice
39 shall consist of all of the following:

1 (A) Email notice when the person or business has an email
2 address for the subject persons.

3 (B) Conspicuous posting of the notice on the Internet Web site
4 page of the person or business, if the person or business maintains
5 one.

6 (C) Notification to major statewide media.

7 (k) Notwithstanding subdivision (j), a person or business that
8 maintains its own notification procedures as part of an information
9 security policy for the treatment of personal information and is
10 otherwise consistent with the timing requirements of this part, shall
11 be deemed to be in compliance with the notification requirements
12 of this section if the person or business notifies subject persons in
13 accordance with its policies in the event of a breach of security of
14 the system.

15 SEC. 3. Title 1.81.23 (commencing with Section 1798.90.5)
16 is added to Part 4 of Division 3 of the Civil Code, to read:

17
18 TITLE 1.81.23. COLLECTION OF LICENSE PLATE
19 INFORMATION
20

21 1798.90.5. The following definitions shall apply for purposes
22 of this title:

23 (a) “Automated license plate recognition end-user” or “ALPR
24 end-user” means a person that accesses or uses ALPR information,
25 but does not include a transportation agency when subject to
26 Section 31490 of the Streets and Highways Code.

27 (b) “Automated license plate recognition information,” or
28 “ALPR information” means information or data collected through
29 the use of an ALPR system.

30 (c) “Automated license plate recognition operator” or “ALPR
31 operator” means a person that operates an ALPR system, or that
32 stores or maintains ALPR information, but does not include a
33 transportation agency when subject to Section 31490 of the Streets
34 and Highways Code.

35 (d) “Automated license plate recognition system” or “ALPR
36 system” means a system of one or more mobile or fixed cameras
37 combined with computer algorithms to read and convert images
38 of registration plates and the characters they contain into
39 computer-readable data.

1 (e) “Person” includes a law enforcement agency, government
2 agency, private entity, or individual.

3 (f) “Public agency” means and includes every state agency and
4 every local agency.

5 1798.90.51. An ALPR operator shall do all of the following:

6 (a) (1) Ensure that ALPR information is protected with
7 reasonable operational, administrative, technical, and physical
8 safeguards to ensure its confidentiality and integrity.

9 (2) Implement and maintain reasonable security procedures and
10 practices in order to protect ALPR information from unauthorized
11 access, destruction, use, modification, or disclosure.

12 (b) (1) Implement and maintain a usage and privacy policy in
13 order to ensure that the ~~collection~~ *collection, use, maintenance,*
14 *sharing, and dissemination* of ALPR information is consistent
15 with respect for individuals’ privacy and civil liberties. The usage
16 and privacy policy shall be available in writing, and, if the ALPR
17 operator has an Internet Web site, the usage and privacy policy
18 shall be posted conspicuously on that Internet Web site.

19 (2) The usage and privacy policy shall, at a minimum, include
20 all of the following:

21 (A) The authorized purposes for using ALPR systems and
22 collecting ALPR information.

23 (B) A description of the employees and independent contractors
24 who are authorized to use ALPR systems, to collect ALPR
25 information, and to access ALPR information. The policy shall
26 identify the training requirements necessary for those authorized
27 employees and independent contractors.

28 (C) A description of how the use of ALPR systems will be
29 monitored to ensure compliance with all applicable privacy laws
30 and a process for periodic system audits, including audits of the
31 access log required by Section 1798.90.52.

32 (D) A description of reasonable measures that will be used to
33 ensure the accuracy of ALPR information and a process to correct
34 data errors.

35 (E) A description of how the ALPR operator will comply with
36 the security procedures and practices implemented and maintained
37 pursuant to subdivision ~~(b)~~ *(a)*.

38 (F) The length of time ALPR information will be stored or
39 retained.

1 (G) The official custodian, or owner, of ALPR information and
2 which employees and independent contractors have the
3 responsibility and accountability for implementing subdivision-(b)
4 (a) and this subdivision.

5 (H) The purpose of, and process for, sharing or disseminating
6 ALPR information with other persons.

7 1798.90.52. If an ALPR operator accesses or provides access
8 to ALPR information, the ALPR operator shall maintain a record
9 of that access. At a minimum, the record shall include all of the
10 following:

11 (a) The date and time the information is accessed.

12 (b) The license plate number or other data elements used to
13 query the ALPR database or system.

14 ~~(c) The person who accesses the information.~~

15 (c) *The name of the person who accesses the information, and,*
16 *as applicable, the organization or entity with whom the person is*
17 *affiliated.*

18 (d) The purpose for accessing the information.

19 1798.90.53. (a) An ALPR end-user shall implement and
20 maintain a usage and privacy policy in order to ensure that the
21 ~~access and use~~ *access, use, sharing, and dissemination* of ALPR
22 information is consistent with respect for individuals' privacy and
23 civil liberties. The usage and privacy policy shall be available in
24 writing, and, if the ALPR end-user has an Internet Web site, the
25 usage and privacy policy shall be posted conspicuously on that
26 Internet Web site.

27 (b) The usage and privacy policy shall, at a minimum, include
28 all of the following:

29 (1) The authorized purposes for accessing and using ALPR
30 information.

31 (2) A description of the employees and independent contractors
32 who are authorized to access and use ALPR information. The
33 policy shall identify the training requirements necessary for those
34 authorized employees and independent contractors.

35 (3) A description of how the access and use of ALPR
36 information will be monitored to ensure compliance with all
37 applicable privacy laws and a process for periodic system audits.

38 (4) The length of time ALPR information will be retained by
39 the ALPR end-user and the process the ALPR end-user will utilize
40 to determine if and when to destroy the retained ALPR information.

1 (5) The official—~~custodian~~ *custodian, or owner*, of ALPR
2 information.

3 (6) The purpose of, and process for, sharing or disseminating
4 ALPR information with other persons.

5 (7) A description of how the end-user will implement reasonable
6 security measures to secure ALPR information from unauthorized
7 access, destruction, use, modification, or disclosure.

8 (8) *Which employees and independent contractors have the*
9 *responsibility and accountability for implementing subdivision (a)*
10 *and this subdivision.*

11 1798.90.54. (a) In addition to any other sanctions, penalties,
12 or remedies provided by law, an individual who has been harmed
13 by a violation of this title may bring a civil action in any court of
14 competent jurisdiction against a person who knowingly caused
15 that violation.

16 (b) The court may award a combination of any one or more of
17 the following:

18 (1) Actual damages, but not less than liquidated damages in the
19 amount of two thousand five hundred dollars (\$2,500).

20 (2) Punitive damages upon proof of willful or reckless disregard
21 of the law.

22 (3) Reasonable attorney's fees and other litigation costs
23 reasonably incurred.

24 (4) Other preliminary and equitable relief as the court determines
25 to be appropriate.

26 1798.90.55. Notwithstanding any other law or regulation, a
27 public agency that considers implementing a program to gather
28 information through the use of an ALPR system shall provide an
29 opportunity for public comment at a regularly scheduled public
30 meeting of the governing body of the public agency before it
31 implements the program.